(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01325 A1

(51) International Patent Classification[7]: G06F 1/00, G07F 7/12

(21) International Application Number: PCT/SE01/01369

(22) International Filing Date: 18 June 2001 (18.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0002416-6 27 June 2000 (27.06.2000) SE

(71) Applicant *(for all designated States except US)*: **TDS TODOS DATA SYSTEM AB** [SE/SE]; Fiskhamnsgatan 2, S-414 58 Göteborg (SE).

(72) Inventor; and

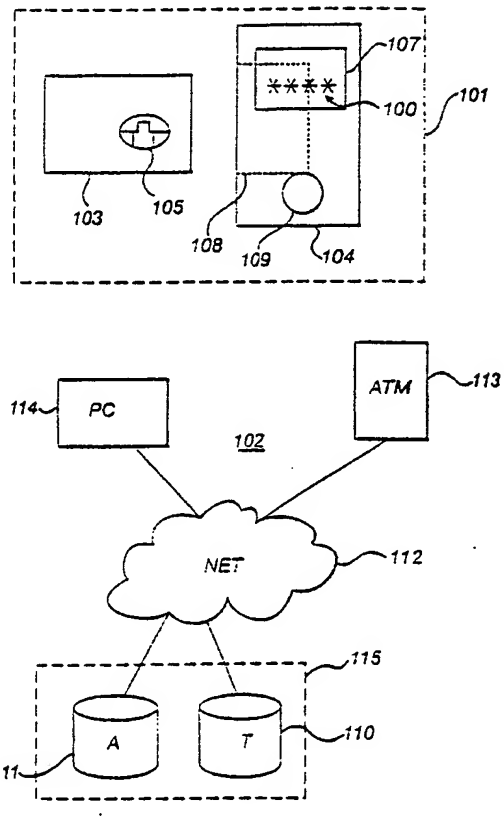
(75) Inventor/Applicant *(for US only)*: JOHANSSON, Anders, O. [SE/SE]; Avstyckningsvägen 40, S-175 50 Järfälla (SE).

(74) Agent: **AWAPATENT AB**; P.O. Box 45086, S-104 30 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: COMMUNICATION METHOD AND DEVICE



(57) Abstract: An authentication arrangement (101), such as a smart card, is identified by an authentication arrangement identification number and communicates with a communication system (102) comprising a transaction manager (110, 111) and an authentication manager (110, 111). The authentication arrangement comprises means for receiving personalizing information from the authentication manager (110, 111) associating the authentication arrangement (101) with the transaction manager (110, 111). Further, the arrangement comprises means for calculating, for a transaction that requires authentication of the user between the user and the transaction manager (110, 111), a substantially non-recurring identification code (100), which depends on the personalizing information. Also comprised in the authentication arrangement are means for supplying the identification code (100) to the user. The user is thereby enabled to authenticate with the transaction manager (110, 111).

WO 02/01325 A1

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

COMMUNICATION METHOD AND DEVICE

TECHNICAL FIELD

The present invention relates to methods and arrangements for secure communication between digital devices. In particular, the invention relates to user authentication in digital communication systems.

BACKGROUND

The need for secure electronic transactions involving a user and a transaction system such as an Internet based shopping site or an automatic teller machine (ATM) at a bank, has increased dramatically during recent years. A major question relating to secure transactions is that of authentication of the user to the system. That is, how to identify a user as being the owner of, e.g., a bank account from which the user is to withdraw money from when using an ATM.

A well-established method of authenticating users in such systems is that of providing the user with an electronically readable device containing information about the user and his account. Such cards are common and contain magnetically stored information. In order to allow the user to use his card in an ATM, the issuer (e.g. the bank) has provided the user with a secret code to be supplied to the ATM when using the card. The code is used "unlock" the card for use by the user every time the user makes use of his card.

A drawback of such a method is that one and the same code is used every time a user authenticates with a system. This increases the risk of unauthorized use of the card if the user loses the card.

An obvious way of avoiding this is to provide systems in which a secret code is used only once, that is for every

transaction the user makes use of a new code. However, this leads to a problem of providing the user with a long list of one-time-codes as well as storing the same list of codes in the system with which the user is to authenticate. Needless to say, such solutions are far from simple to administrate due to the fact that it calls for large storage areas in the authentication system, as well as being insecure due to the fact that the user holds a list of codes to be used in the future.

A problem to solve, in the field of user authentication, is hence how to provide users and authentication- and transaction managers with a more flexible solution which also increases security when making transactions in digital communication networks.

SUMMARY OF THE INVENTION

An object of the present invention is to solve the problem as stated above. To that end, methods and arrangements are provided as stated in the appended claims.

In short, an authentication arrangement, such as a personal smart card or IC-card comprising processing means, memory means and communication means, is used together with a reader capable of reading out information from the authentication arrangement. The authentication arrangement generates, e.g. as a response to a signal from the reader, a one-time identification code that is used by the user to authenticate himself when making transactions via a digital network. A typical example of such a transaction is the use of an ATM when withdrawing money from a bank account.

In some more detail, the invention can be seen in different aspects. A first aspect as seen from the point-of-view of the user possessing a smart card. In a second aspect from the point-of-view of a transaction manager or authentication manager, in the form of one or more

computers in a system or network, at a bank for example, communicating with the user when he/she is performing the transactions. Both of these aspects of the invention will be summarized below.

A method and a system for user authentication in a digital communication system are provided. The communication system comprises a transaction manager and an authentication manager, both of which may be separate functional units in one computer or functional units in different computers.

The user possesses an authentication arrangement, such as a smart card, which is identified by an authentication arrangement identification number. Personalizing information is supplied to the authentication arrangement, preferably by a supplier who is closely related to the authentication manager and/or the transaction manager. The personalizing information associates the authentication arrangement held by the user with the transaction manager. Advantageously, there may be a number of different sets of personalizing information, supplied by a number of different authentication or transaction managers. Such a case enables a user to use one and the same authentication arrangement when making transactions with different transaction managers.

For each transaction the user performs which requires authentication, the system in the form of an authentication manager receives at least one substantially non-recurring identification code. The identification code has been generated by the user authentication arrangement and is dependent on the personalizing information. Hence the identification code is acting as a unique, one-time, signature that identifies the user as being the authorized one.

The reception of the code may take place by means of a direct communication channel between the authentication

manager and the authentication arrangement. A typical example of such a case is when the authentication arrangement, e.g. a smart card, is used in connection with an ATM where a smart card is inserted by the user whereupon the smart card calculates and submits the identification code to, e.g., the bank. The reception of the identification code may also take place in connection with a transaction where the user himself submits the identification code when communicating with, e.g., a web-based shop. A transaction taking place in such a case may involve the user using a separate portable card reader comprising a display on which the identification code is displayed after having been calculated by the smart card hardware.

When receiving the identification code from the user, the authentication manager also computes a substantially non-recurring code. This code is a verification code, which also is dependent on the personalizing information previously supplied to the authentication arrangement. The authentication manager then performs a process of verifying that the received identification code is equal to the calculated verification code. This may simply be performed as a comparison between the two codes. In the case the codes match the user is authenticated and should be allowed to perform the transaction with the system.

Preferably, during a transaction between the user authentication arrangement and the authentication system, the authentication system obtains information regarding the identity of the authentication arrangement, i.e. the identification number, together with a transaction sequence number. The identification number may be transmitted from the user authentication arrangement during the transaction. However, the sequence number need not be transmitted during the transaction. Preferably, a current sequence number which is associated with the particular user authentication arrangement making the

transaction, may be kept at the authentication system and need not be transmitted from the user authentication arrangement.

These two numbers are encrypted by the smart card using two encryption keys contained in the personalizing information previously supplied by the authentication arrangement, e.g. when the user registers himself as a customer and obtains his smart card from a party who controls the authentication- or transaction system. Thus generating a substantially non-recurring identification code.

Since the transaction sequence number is calculated independently by the user authentication arrangement and the authentication system, these two numbers may get unsynchronized. In such a case the authentication system may calculate a value for the verification code which is erroneous. In stead of concluding that the user is unauthorized, the authentication system may attempt to adjust the transaction sequence number and calculate a new verification code to be compared with the received identification code. This adjustment may take place an arbitrary number of times.

A preferred embodiment of the invention is in the form of a personal smart card, as claimed below. The smart card may be used together with a portable card reader as will be discussed below.

With respect to all aspects of the invention, computer software implementation is obviously preferred. The software of the authentication- and transaction managers may be present in more or less traditional computers, and the software of the user authentication arrangement may be within smart cards or other portable units having processing- and storage means. To that end, inventive subjects in the form of computer programs are also to be found among the claims.

There are a number of advantages of the present invention, including the fact that there are the secret keys are kept inside the authentication arrangement, thus increasing the security.

Another advantage is that it is possible for a user to use different readers with his/her smart card, thus making it flexible in terms of use in different locations. Conversely, several users can use one and the same reader, each user having his/her own personal smart card. Also, a user may have multiple sets of personalizing information all of which are associated with, and preferably also obtained from, different transaction- or authentication managers belonging to, e.g., different banks.

Yet another advantage is that the minimum amount of data which has to be kept at the authentication manager computer site. For example, no large table of sequences of identification codes, that may occupy large storage areas, is needed.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates schematically a system according to the present invention.

Figure 2 illustrates schematically a personalizing procedure according to the present invention.

Figure 3 illustrates schematically a procedure for identification code generation according to the present invention.

Figure 4 illustrates schematically a verification procedure according to the present invention.

PREFERRED EMBODIMENTS

In figure 1 a user authentication arrangement in the form of a smart card 103, or integrated circuit card (ICC), and portable card reader 104 acts together to provide a

user with a one-time identification code. The card 103 comprises smart card hardware 105 as known in the art, which connects electrically via a slot 108 in the reader 104. A push button 109 on the reader 104 initiates software in the card 103 to calculate the identification code and transfer it to the reader 104, which in turn displays the code in the form of a four-digit number 100 on a display 107. Obviously, any number of digits or other character may be generated. That is, the invention is not restricted to "traditional" four-digit identification codes.

A system 102 with which the user or the smart card communicates comprises a computer 114 and an automatic teller machine 113 (ATM). These two units are connected via a computer network 112 to a transaction manager 110 and an authentication manager 111, both of which may be physically separated or, as indicated by a dashed line 115, joined in one and the same physical unit, as the skilled person realizes.

With reference to the system 102 in figure 1 and schematic flow diagrams in figures 2 to 4 a preferred embodiment of the invention will now be described.

The user holding the card, or rather the smart card itself, is in figure 2 associated with a transaction manager or authentication manager. The association may simply mean establishing a business relation such as the user obtaining a banking card from a bank. Figure 2 specifically illustrates the steps of personalizing the card before it is to be used to authenticate the user in a transaction. A unique identification number 201, e.g. a card number comprising a number of digits, is subject to encryption algorithms 204 and 206 using derivation keys 203 and 205 respectively. Two different encrypting keys 207 and 209 are generated. These encryption keys are in turn encrypted in steps 212 and 214 using keys 211 and 213 respectively for the purpose of enabling a secure

transport to a functional unit 215 (personalizing unit 215), which may be located at a site different from where the above steps are performed. The personalizing unit 215 decrypts in steps 218 and 219 the transported encryption keys 207 and 209, by using transport decryption keys 216 and 217 respectively, and stores them in the smart card 200 by way of a writing step (not shown). The card 200 is by this process personalized. That is, an association is made between the user and the transaction- or authentication manager which performed the personalizing process.

When the user is to perform a transaction with a transaction manager, he must supply an identification code together with, as is known in the art, other information relating to the transaction. Referring to figure 3, the identification number 301 of the smart card and a transaction sequence number 303 are encrypted in steps 306 and 308. An XOR operation between the sequence number and the identification number 301 is performed in order to introduce a non-static dynamic property of the encryption step 308. The encryption 306,308 is performed using the encryption keys 305 and 307 stored in the card by the personalizing process described above in connection with figure 2. The output of the encrypting steps 306,308 are combined in a logical XOR-step 311 in order to ensure that the generated identification code is made dependent on both encryption steps 306 and 308. A resulting bit sequence is converted into a decimal number, such as a four digit number, in step 313 and supplied in step 315. The supplying of the identification may be either by way of presenting it on the display 107 of the card reader 104. The identification code may also be directly supplied via, e.g., the ATM to the transaction manager. The sequence number is incremented and stored for use in further transactions.

Referring now to figure 4, from the point of view of the authentication manager, the received identification code

401 is compared in a comparison step 411 with a calculated verification code generated in a verification code generation step 409. The verification code is calculated in steps 403 and 409 using derivation keys 402 and the identification number 404 of the smart card, in the same way as the identification code was calculated in the processing means of the smart card, as described above in connection with figure 3. The identification number of the smart card is preferably also received together with the identification code. However, the number of the card may be "indirectly" received by means of a pointer to a database of card numbers at the authentication manager. The verification code and the received identification code are compared in step 411. If they are equal, the user is considered authenticated and allowed to proceed with the transaction as indicated by step 414. If the verification code and the received identification code differ, the situation may be that an identification code has been supplied which has not been generated by a personalized smart card, in which case the transaction is not to be allowed. However, the comparison may also result in an inequality if the transaction sequence numbers that have been used to generate the identification code and the verification code, in the smart card and the authentication manager respectively, are different. This may occur if there have been interrupted transactions where the sequence number of the smart card has been incremented without the identification code being received by the authentication manager. In such a situation, the sequence number may be adjusted in an adjustment step 417 and a new verification code may be calculated. This adjustment and re-calculation may be performed an arbitrary number of times as indicated by a decision step 413 where it is decided whether or not a re-calculation based on a different sequence number should be allowed. Final step 415 then

indicates that the user is not authenticated to the system.

CLAIMS

1. A method for authenticating a user in a digital communication system (102), the communication system (102) comprising a transaction manager (110,111) and an authentication manager (110,111), the user possessing an authentication arrangement (101) being identified by an authentication arrangement identification number, comprising:

- supplying personalizing information to the authentication arrangement (101), said personalizing information associating the authentication arrangement (101) with the at least one transaction manager (110,111),

- receiving, for each transaction of a plurality of transactions requiring authentication of the user between the user and the at least one transaction manager (110,111), at least one substantially non-recurring identification code (100), the identification code being dependent on the personalizing information,

- calculating, for each transaction of a plurality of transactions requiring authentication of the user between the user and the at least one transaction manager (110,111), at least one substantially non-recurring verification code, the identification code being dependent on the personalizing information supplied to the authentication arrangement (101),

- verifying, for each transaction of a plurality of transactions requiring authentication of the user between the user and the at least one transaction manager (110,111), comprising a comparison between the received identification code (100) and the calculated verification code, thereby authenticating the user to the system (102).

2. A method according to claim 1, where receiving the identification code comprises receiving the

authentication arrangement identification number and a transaction sequence number in encrypted form.

3. A method according to claim 1 or 2, where supplying personalizing information comprises supplying at least a first key and a second key.

4. A method according to claim 3, where receiving the identification code comprises receiving the authentication arrangement identification number encrypted by the first key and receiving the transaction sequence number encrypted by the second key.

5. A method according to claim 2, where the steps of calculating and verifying comprises adjusting the transaction sequence number.

6. A method according to claim 5, where the adjusting comprises at least one of adding and subtracting the transaction sequence number.

7. An authentication system (115) for authenticating a user in a digital communication system (102), the communication system (102) comprising a transaction manager (110,111) and an authentication manager (110,111), the user possessing an authentication arrangement (101) being identified by an authentication arrangement identification number, comprising:

- means for supplying personalizing information to the authentication arrangement (101), said personalizing information associating the authentication arrangement (101) with the transaction manager (110,111),

- means for receiving, for each transaction of a plurality of transactions requiring authentication of the user between the user and the transaction manager (110,111), at least one substantially non-recurring identification code (100), the identification code being dependent on the personalizing information,

- means for calculating, for each transaction of a plurality of transactions requiring authentication of the

user between the user and the transaction manager (110,111), at least one substantially non-recurring verification code, the verification code being dependent on the personalizing information supplied to the authentication arrangement (101),

- means for verifying, for each transaction of a plurality of transactions requiring authentication of the user between the user and the transaction manager (110,111), comprising means for comparing the received identification code (100) and the calculated verification code, thereby authenticating the user to the transaction manager (110,111).

8. An arrangement according to claim 7, where the means for receiving the identification code comprises means for receiving the authentication arrangement identification number and a transaction sequence number in encrypted form.

9. An arrangement according to claim 7 or 8, where the means for supplying personalizing information comprises means for supplying at least a first key and a second key.

10. An arrangement according to claim 9, where the means for receiving the identification code comprises means for receiving the authentication arrangement identification number encrypted by the first key and means for receiving the transaction sequence number encrypted by the second key.

11. An arrangement according to claim 8, where the means for calculating and verifying comprises means for adjusting the transaction sequence number.

12. An arrangement according to claim 11, where the adjusting comprises at least one of means for adding and means for subtracting the transaction sequence number.

13. A method for enabling user authentication in a digital communication system (102), the communication

system (102) comprising a transaction manager (110,111) and an authentication manager (110,111), the user possessing an authentication arrangement (101), the authentication arrangement (101) being identified by an authentication arrangement identification number, comprising:

- receiving personalizing information in the authentication arrangement (101) from the authentication manager (110,111), said personalizing information associating the authentication arrangement (101) with the transaction manager (110,111),

- calculating, for each transaction of a plurality of transactions requiring authentication of the user between the user and the transaction manager (110,111), at least one substantially non-recurring identification code (100), the identification code being dependent on the personalizing information,

- supplying the at least one identification code (100) to the user, thereby enabling user authentication with the transaction manager (110,111), or supplying the at least one identification code (100) to the authentication manager (110,111), thereby enabling user authentication with the transaction manager (110,111).

14. A method according to claim 13, where calculating the identification code comprises encrypting the authentication arrangement identification number and a transaction sequence number.

15. A method according to claim 13 or 14, where receiving personalizing information in the authentication arrangement (101) comprises receiving at least a first key and a second key.

16. A method according to claim 15, where calculating the identification code comprises encrypting the authentication arrangement identification number using the first key and encrypting the transaction sequence number using the second key.

17. A method according to any one of claims 13-16, further comprising:

- enabling the authentication arrangement (101) by receiving and processing an unlocking code.

18. An authentication arrangement (101) for authenticating a user in a digital communication system (102), the authentication arrangement (101) being identified by an authentication arrangement identification number and the communication system (102) comprising a transaction manager (110,111) and an authentication manager (110,111), comprising:

- means for receiving personalizing information from the authentication manager (110,111), said personalizing information associating the authentication arrangement (101) with the transaction manager (110,111),

- means for calculating, for each transaction of a plurality of transactions requiring authentication of the user between the user and the transaction manager (110,111), at least one substantially non-recurring identification code (100), the identification code being dependent on the personalizing information,

- means for supplying the at least one identification code (100) to the user, thereby enabling user authentication with the transaction manager (110,111), or means for supplying the at least one identification code (100) to the authentication manager (110,111), thereby enabling user authentication with the transaction manager (110,111).

19. An arrangement according to claim 18, where the means for calculating the identification code comprises means for encrypting the authentication arrangement identification number and a transaction sequence number.

20. An arrangement according to claim 18 or 19, where the means for receiving personalizing information in the authentication arrangement (101) comprises means for receiving at least a first key and a second key.

21. An arrangement according to claim 20, where the means for calculating the identification code comprises means for encrypting the authentication arrangement identification number using the first key and means for encrypting the transaction sequence number using the second key.

22. An arrangement according to any one of claims 18-21, further comprising:

- means for enabling the authentication arrangement (101) comprising means for receiving and processing an unlocking code.

23. An arrangement according to any one of claims 18-22, further comprising:

- means for controlling a plurality of different sets of personalizing information, said sets being associated with at least a respective transaction manager (110,111).

24. An arrangement according to any one of claims 18-23, comprising means for communicating with a reader arrangement (104).

25. A computer program, comprising software instructions performing a method according to any of claims 1-9.

26. A computer program, comprising software instructions performing a method according to any of claims 13-17.

27. A smart-card (103) for authenticating a user in a digital communication system (102), the smart-card (103) being identified by a smart-card identification number and the communication system (102) comprising a transaction manager (110,111) and an authentication manager (110,111), comprising:

- means for receiving personalizing information from the authentication manager (110,111), said personalizing information associating the smart-card (103) with the transaction manager (110,111),

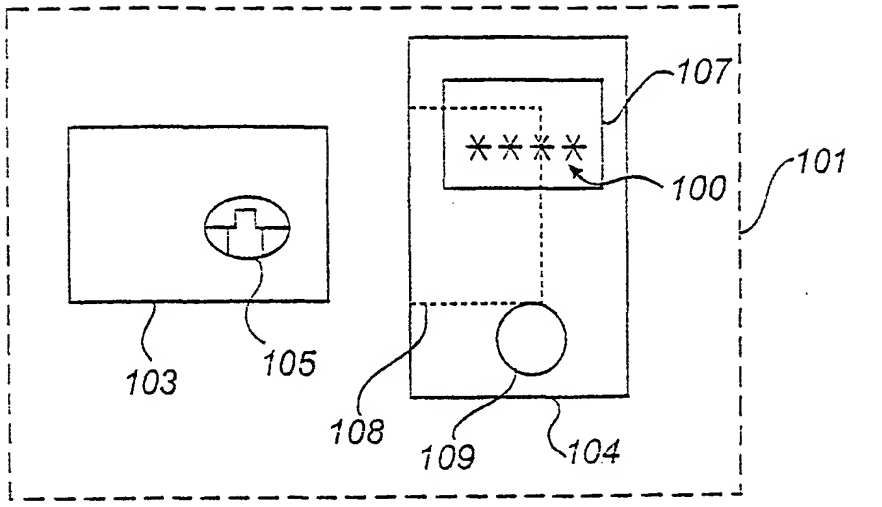
- means for calculating, for each transaction of a

plurality of transactions requiring authentication of the user between the user and the transaction manager (110,111), at least one substantially non-recurring identification code (100), the identification code being dependent on the personalizing information,

- means for supplying the at least one identification code (100) to the authentication manager (110,111), thereby authenticating the user to the transaction manager (110,111).

28. A smart-card according to claim 27, comprising means for communicating with a card reader (104).

29. A smart-card reader comprising means for communicating with a smart-card according to any one of claims 27-28.


107
100
101
103
105
108
109
104

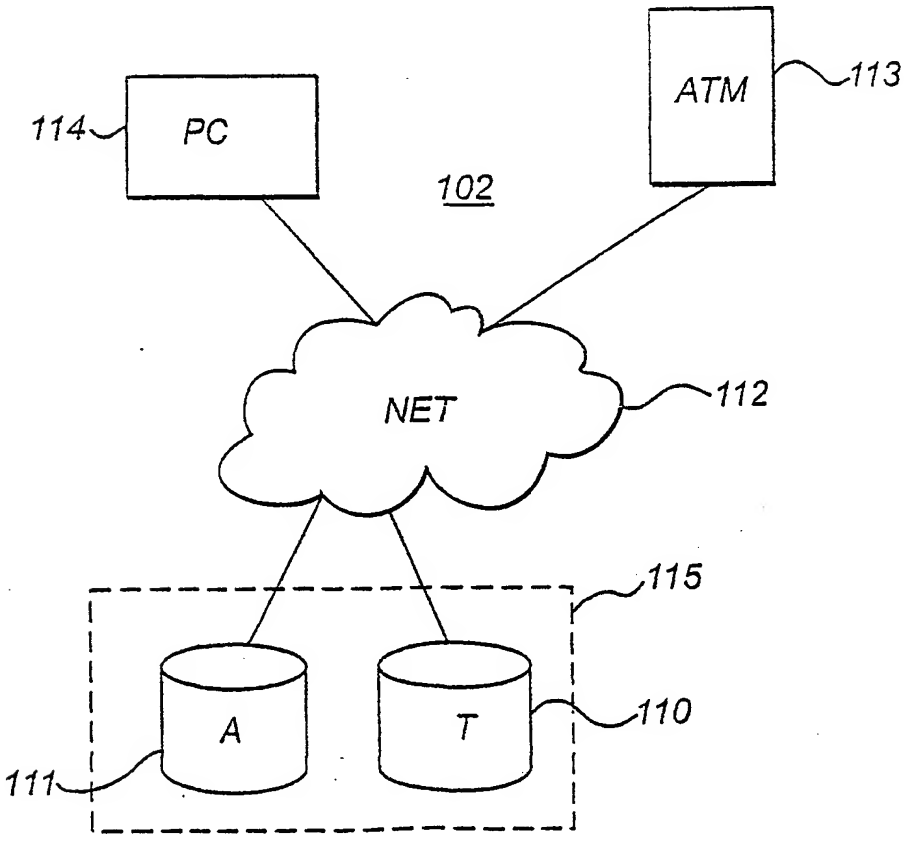

ATM
113
114
PC
102
NET
112
115
A
T
110
111

Fig. 1

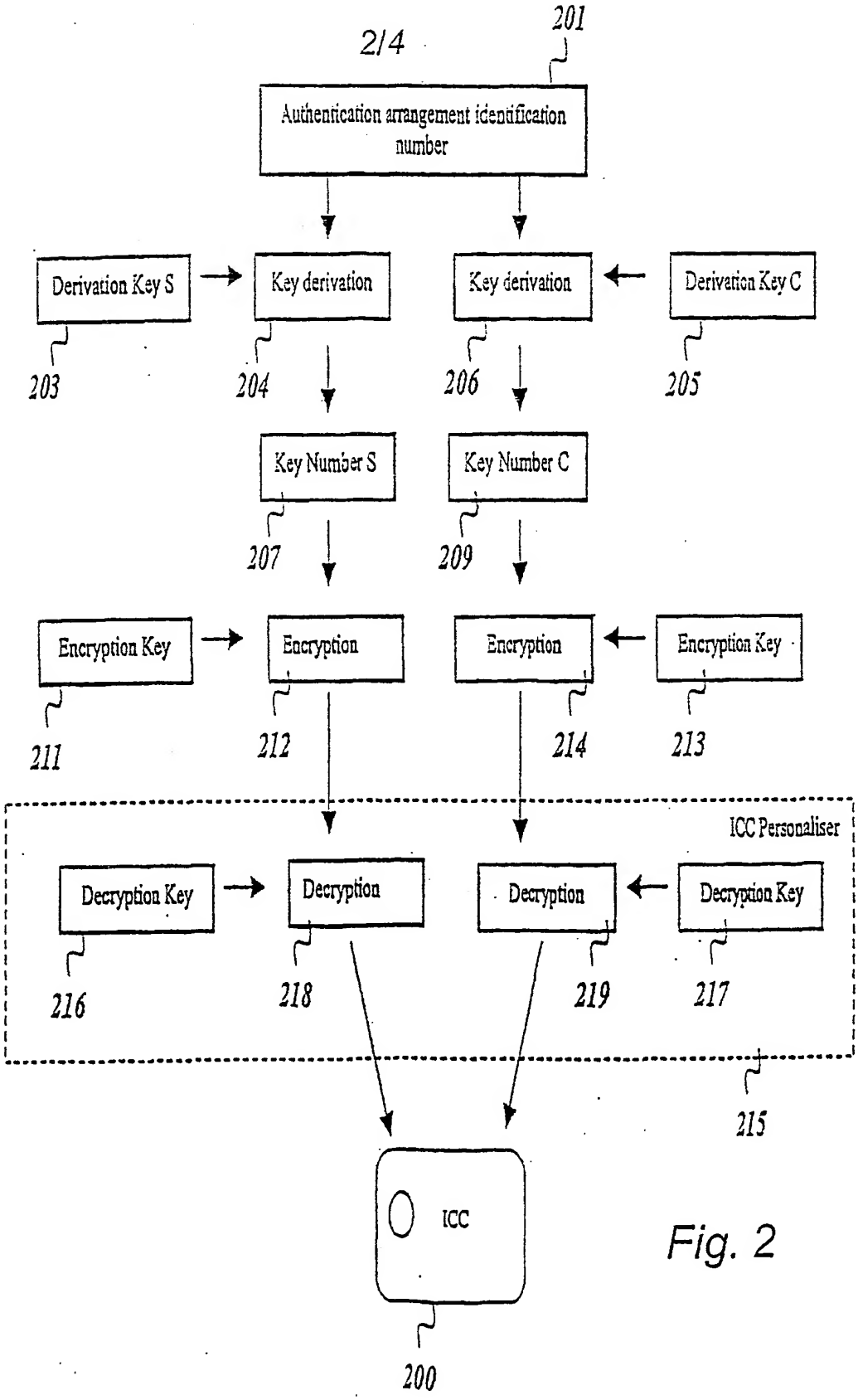

214
201
Authentication arrangement identification number
Derivation Key S
Key derivation
Key derivation
Derivation Key C
203
204
206
205
Key Number S
Key Number C
207
209
Encryption Key
Encryption
Encryption
Encryption Key
211
212
214
213
ICC Personaliser
Decryption Key
Decryption
Decryption
Decryption Key
216
218
219
217
215
ICC
200

Fig. 2

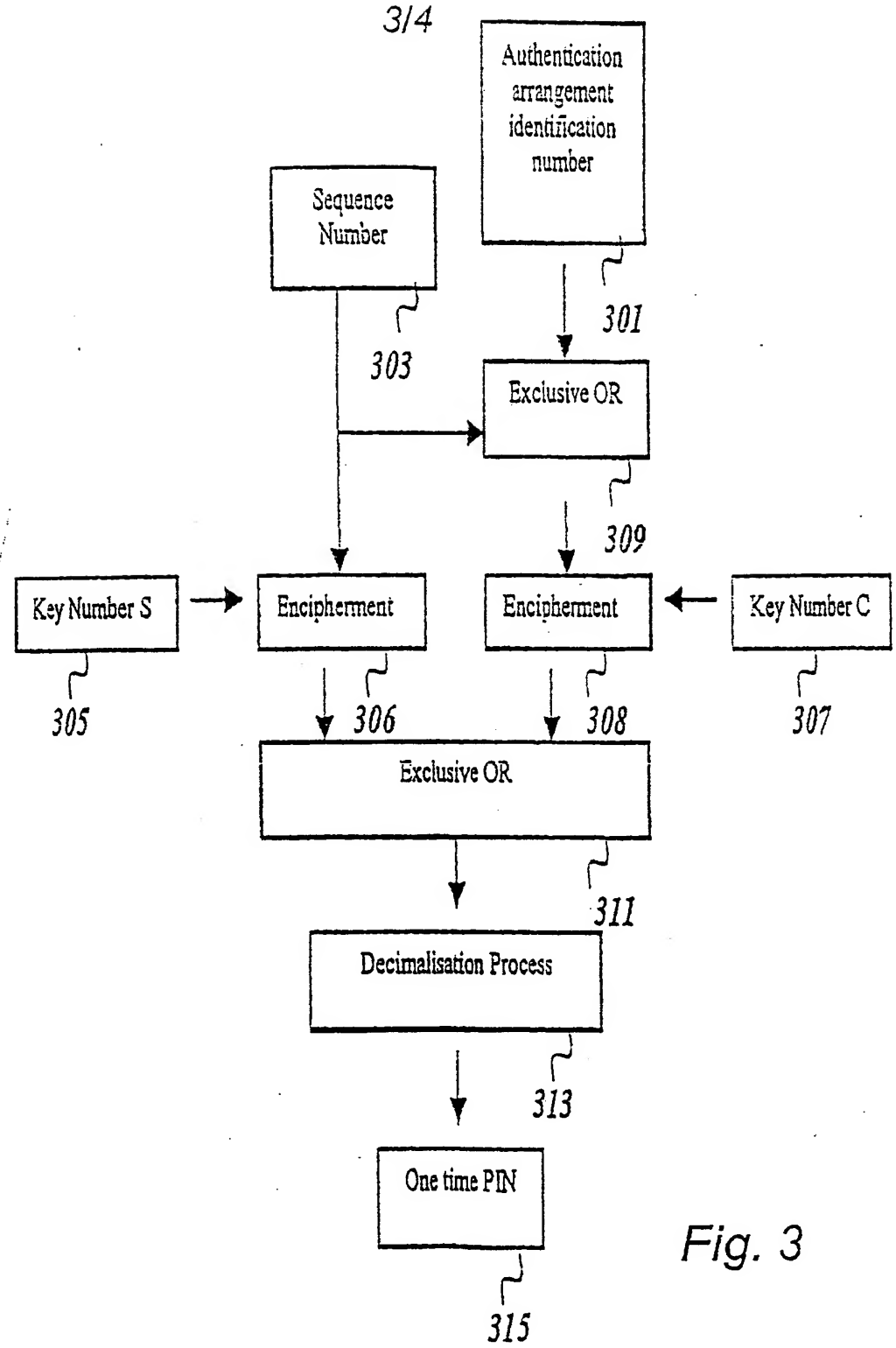

Authentication arrangement identification number
Sequence Number
301
303
Exclusive OR
309
Key Number S
Encipherment
Encipherment
Key Number C
305
306
308
307
Exclusive OR
311
Decimalisation Process
313
One time PIN
315

Fig. 3

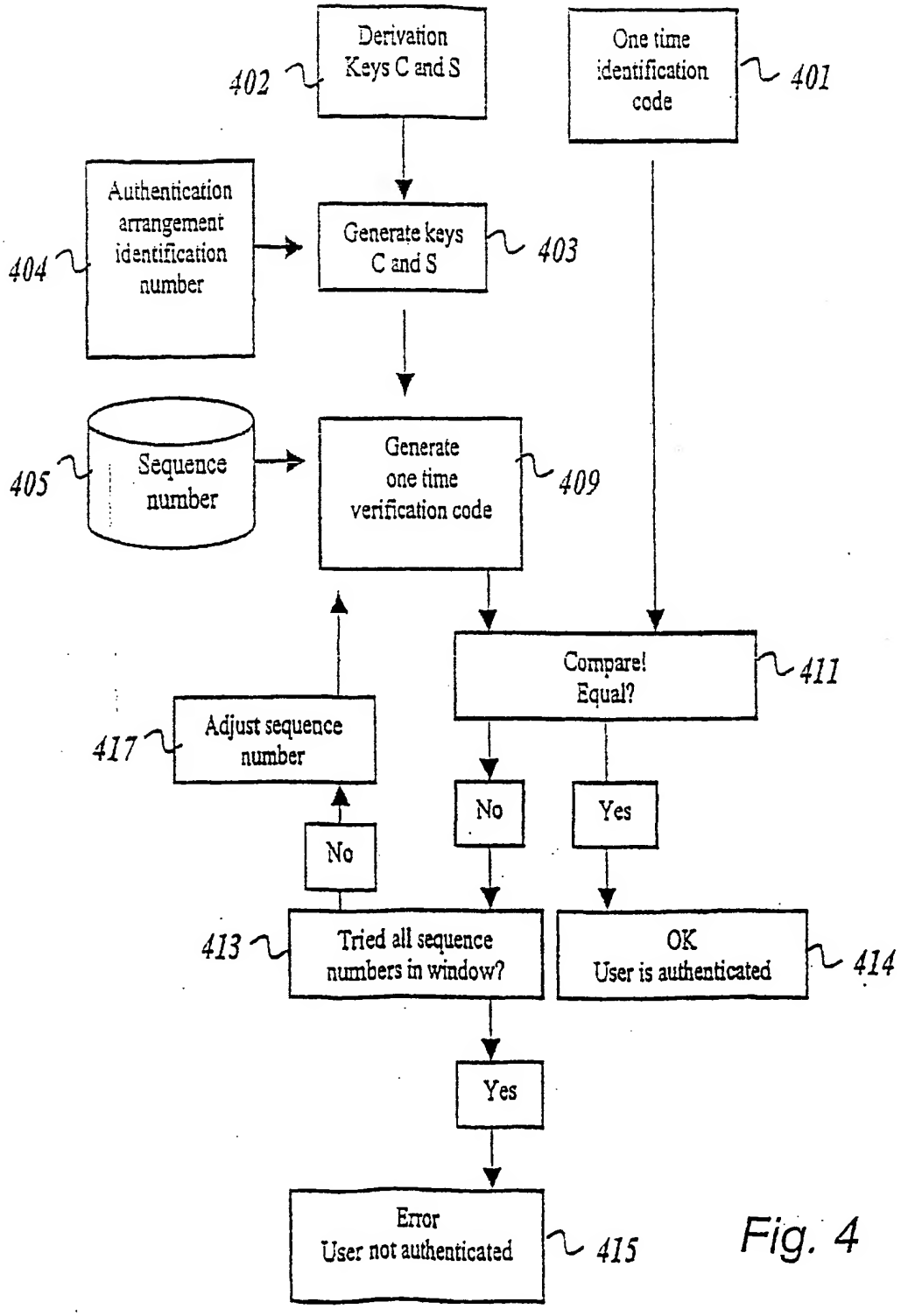

Derivation Keys C and S
402
One time identification code
401
Authentication arrangement identification number
404
Generate keys C and S
403
Sequence number
405
Generate one time verification code
409
Compare! Equal?
411
Adjust sequence number
417
No
Yes
No
Tried all sequence numbers in window?
413
OK User is authenticated
414
Yes
Error User not authenticated
415

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01369

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, G07F 7/12
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	D1:HEIMDAL, Pär; Investigations over a Payment and Authentication System based on Smart Cards; Stockholm: Kungliga Tekniska Högskolan, Institutionen för Data- och Systemvetenskap, Electrum 230, 164 40 Kista; November 1999; pages 38-46. See pages 38-41	1-29
	--	
X	EP 0427465 A2 (AMERICAN TELEPHONE AND TELEGRAPH COMPANY), 15 May 1991 (15.05.91), column 3, line 21 - column 4, line 17; column 12, line 31 - column 13, line 28, figure 1, claim 1, abstract	1-29
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 October 2001	29 -10- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Pär Heimdal/LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01369

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0723251 A2 (TANDEM COMPUTERS INCORPORATED), 24 July 1996 (24.07.96), page 2, line 49 - page 3, line 54, claim 1, abstract --	1-29
X	EP 0867843 A2 (SONY CORPORATION), 30 Sept 1998 (30.09.98), column 2, line 11 - column 6, line 34, claims 1-5, abstract --	1-29
X	WO 9514968 A1 (FORTRESS U & T LTD.), 1 June 1995 (01.06.95), page 1, line 1 - page 5, line 5; page 6, line 25 - page 8, line 16, figures 7-9, claim 1, abstract --	1-29
X	EP 0998073 A2 (MATSUSHITA ELECTRIC INDUSTRIAL CO LTD), 3 May 2000 (03.05.00), column 5, line 31 - column 6, line 21, claim 1, abstract --	1-29
A	A 6073238 US (MICHEL MARCO PAUL DRUPSTEEN), 6 June 2000 (06.06.00), column 1, line 44 - column 2, line 10, figure 3, claim 1, abstract -- --------	1-29

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/10/01

International application No.
PCT/SE 01/01369

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0427465 A2	15/05/91	CA 2023872 A,C	10/05/91
		DE 69016589 D,T	07/09/95
		JP 1921556 C	07/04/95
		JP 3158955 A	08/07/91
		JP 6052518 B	06/07/94
		US 5120939 A	09/06/92
EP 0723251 A2	24/07/96	CA 2167631 A	21/07/96
		US 5757918 A	26/05/98
EP 0867843 A2	30/09/98	JP 10327142 A	08/12/98
		TW 423242 B	00/00/00
		US 6058477 A	02/05/00
WO 9514968 A1	01/06/95	EP 0731941 A	18/09/96
		IL 107789 D	00/00/00
EP 0998073 A2	03/05/00	JP 2000138674 A	16/05/00
		JP 3015362 B	06/03/00
		JP 2000196588 A	14/07/00
A 6073238 US	06/06/00	NONE	